PDR RID Report

Date Last Modified 7/6/95

Originator Gaylord, Arthur S. **Phone No** 413-545-2520

Organization Project Pilgrim, Univ. of Massachusetts

E Mail Address art@cs.umass.edu

Document CSMS Requirements Spec (304-CD-003-001)

Section 5.2.4.5 **Page** 5-41 **Figure Table** NA

RID ID PDR 197

Review CSMS

Originator Ref

Priority 2

Category Name Requirements **Actionee** HAIS

Sub Category

Subject Intrusion Detection and reporting requirements

Description of Problem or Suggestion:

The specifications only details the requirements for periodic checking for security audit trails. I suggest considering more active measures such as secure, real-time reporting of security alerts (possibly via out-of-band communications channels) and some degree of intrusion avoidance counter measures, such the deactivation of accounts under attack, etc. Also, care should be taken to detect denial of service attacks and react to them, especially for key services such security, naming, and event services. One of the ISS specifications includes network router based counter measures, but this is insufficient to protect against attacks internal to a LAN.

Originator's Recommendation

Consider and revise requirements if deemed appropriate.

GSFC Response by: **GSFC Response Date**

HAIS Response by: Forman **HAIS Schedule** 2/28/95

HAIS R. E. Y Sastry **HAIS Response Date** 6/27/95

The mechanism for the real-time notification of events (including security events) exists and is described in section 5.4.1.2. The referenced section, Section 5.2.4.5 discusses the capability for browsing the log files/security audit trail which supports non real-time correlation of events to identify potential security threats which may not be independently detected. Denial of service will be detected and reported in real time, alerts or alarms associated with such reports will be configurable.

Status **Closed** **Date Closed** **7/6/95** **Sponsor** **Broder**

****** **Attachment if any** ******